日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　８月１８日

出願番号
Application Number: 特願２００３－２９４１０１

[ST. 10/C]: [ＪＰ２００３－２９４１０１]

出願人
Applicant(s): ＦＤＫ株式会社

２００３年１０月３１日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

【書類名】　特許願
【整理番号】　IP03533
【あて先】　特許庁長官　殿
【国際特許分類】　G06F　7/58
【発明者】
　【住所又は居所】　東京都港区新橋５丁目３６番１１号　エフ・ディー・ケイ株式会社内
　【氏名】　山本　博康
【発明者】
　【住所又は居所】　東京都港区新橋５丁目３６番１１号　エフ・ディー・ケイ株式会社内
　【氏名】　中野　初美
【発明者】
　【住所又は居所】　東京都港区新橋５丁目３６番１１号　エフ・ディー・ケイ株式会社内
　【氏名】　清水　隆邦
【発明者】
　【住所又は居所】　東京都港区新橋５丁目３６番１１号　エフ・ディー・ケイ株式会社内
　【氏名】　アナンダ　ビターナゲ
【発明者】
　【住所又は居所】　東京都港区新橋５丁目３６番１１号　エフ・ディー・ケイ株式会社内
　【氏名】　鯉渕　美佐子
【特許出願人】
　【識別番号】　000237721
　【氏名又は名称】　エフ・ディー・ケイ株式会社
【代理人】
　【識別番号】　100096862
　【弁理士】
　【氏名又は名称】　清水　千春
　【電話番号】　03-3543-0036
【選任した代理人】
　【識別番号】　100067046
　【弁理士】
　【氏名又は名称】　尾股　行雄
　【電話番号】　03-3543-0036
【手数料の表示】
　【予納台帳番号】　057761
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
抵抗およびキャパシタでクロック信号を積分して積分波形を出力する積分回路と、ノイズ源と、このノイズ源のノイズを増幅してノイズ信号を出力するアンプと、前記積分波形と前記ノイズ信号とをミキシングするミキサーと、このミキサーの出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路とを２個ずつ備え、
前記各エッジ検出回路の出力信号の位相差に基づいて“０”または“１”を出力するフリップ・フロップを備え、
前記各積分回路に入力される入力信号の位相を調整するディレー、第１セレクターおよびアップ／ダウンカウンターからなる位相調整部を備え、
前記フリップ・フロップから出力される“０”または“１”がそれぞれ５０％に収束するように当該フリップ・フロップの出力を前記位相調整部にフィードバックするフィードバック回路を備えた物理乱数発生器において、
前記各積分回路の前段にそれぞれ第２セレクターおよび第３セレクターを設け、
前記アップ／ダウンカウンターの最上位ビットによって前記第１セレクターと前記第２セレクターおよび前記第３セレクターとの入力の極性切換を行う極性切換回路を設けたことを特徴とする物理乱数発生器。
【請求項２】
抵抗およびキャパシタでクロック信号を積分して積分波形を出力する積分回路を１つ備え、
ノイズ源と、このノイズ源のノイズを増幅してノイズ信号を出力するアンプと、前記積分波形と前記ノイズ信号とをミキシングするミキサーと、このミキサーの出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路とを２個ずつ備え、
前記各エッジ検出回路の出力信号の位相差に基づいて“０”または“１”を出力するフリップ・フロップを備えた物理乱数発生器において、
前記フリップ・フロップに入力される入力信号の位相を調整するディレーとセレクターからなる可変ディレーを前記各エッジ検出回路の前段または後段に設け、
前記フリップ・フロップから出力される“０”または“１”がそれぞれ５０％に収束するように当該フリップ・フロップの出力を前記可変ディレーにフィードバックするフィードバック回路を設けたことを特徴とする物理乱数発生器。
【請求項３】
前記積分回路の抵抗の後段にＦＥＴを当該積分回路のキャパシタと並列に付加したことを特徴とする請求項１または請求項２に記載の物理乱数発生器。
【請求項４】
前記積分回路の抵抗に代えて定電流回路を設けたことを特徴とする請求項１から請求項３までのいずれかに記載の物理乱数発生器。
【請求項５】
請求項１から請求項４までのいずれかに記載の物理乱数発生器を２個以上並列接続し、前記各物理乱数発生器に入力されたパラレル物理乱数をシリアル物理乱数に並べ替えて出力するようにしたことを特徴とする物理乱数発生装置。

【書類名】明細書
【発明の名称】物理乱数発生器および物理乱数発生装置
【技術分野】
【０００１】
本発明は、各種の用途に用いるに好適な物理乱数発生器および物理乱数発生装置に関するものであり、その具体的な用途としては、セキュリティー、暗号、認証、施錠、暗号化通信、スマートカード（例えば、電子マネー、クレジットカード、診察券）、ホームセキュリティー、カーセキュリティー、キーレスエントリー、確率、抽選、ゲーム、アミューズメント（例えば、パチンコ、パチスロ）、シミュレーション（例えば、気象・学術計算・株価におけるモンテカルロ）、グラフィックス（例えば、ＣＧ、自動作曲）、制御、計測、ＦＡ、ロボット制御（人工知能）などが挙げられる。
【背景技術】
【０００２】
従来この種の物理乱数発生装置としては、例えば特許文献１に開示されているように、２個のディレーおよびセレクター等からなる位相調整部と、フリップ・フロップと、フィードバック回路とから構成される物理乱数発生器を備えたものが知られている。
【特許文献１】特開２００３－２９９６４号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
しかし、これでは、フリップ・フロップのクロック端子とデータ端子に入力される２系統の信号ラインに応じた２個のディレーおよびセレクターが必要となるので、位相調整部、ひいては物理乱数発生器の規模が大きくなり、その占有面積が拡大するばかりか、その消費電力が増大するという不都合があった。特に、物理乱数発生器がＣＰＵ（中央演算処理装置）、ＲＯＭ（読取り専用記憶装置）、ＲＡＭ（読取り書込み記憶装置）などの多くの機能とＩＣ（集積回路）内に混載される場合には、この物理乱数発生器の占有面積をできる限り縮小することが強く望まれる。
【０００４】
本発明は、このような事情に鑑み、占有面積が小さくて消費電力が少ない物理乱数発生器と、この物理乱数発生器が組み込まれた物理乱数発生装置を提供することを目的とする。
【課題を解決するための手段】
【０００５】
まず、本発明のうち請求項１に係る発明は、抵抗およびキャパシタでクロック信号を積分して積分波形を出力する積分回路と、ノイズ源と、このノイズ源のノイズを増幅してノイズ信号を出力するアンプと、前記積分波形と前記ノイズ信号とをミキシングするミキサーと、このミキサーの出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路とを２個ずつ備え、前記各エッジ検出回路の出力信号の位相差に基づいて“０”または“１”を出力するフリップ・フロップを備え、前記各積分回路に入力される入力信号の位相を調整するディレー、第１セレクターおよびアップ／ダウンカウンターからなる位相調整部を備え、前記フリップ・フロップから出力される“０”または“１”がそれぞれ５０％に収束するように当該フリップ・フロップの出力を前記位相調整部にフィードバックするフィードバック回路を備えた物理乱数発生器において、前記各積分回路の前段にそれぞれ第２セレクターおよび第３セレクターを設け、前記アップ／ダウンカウンターの最上位ビットによって前記第１セレクターと前記第２セレクターおよび前記第３セレクターとの入力の極性切換を行う極性切換回路を設けて構成される。
【０００６】
また、本発明のうち請求項２に係る発明は、抵抗およびキャパシタでクロック信号を積分して積分波形を出力する積分回路を１つ備え、ノイズ源と、このノイズ源のノイズを増幅してノイズ信号を出力するアンプと、前記積分波形と前記ノイズ信号とをミキシングす

るミキサーと、このミキサーの出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路とを２個ずつ備え、前記各エッジ検出回路の出力信号の位相差に基づいて“０”または“１”を出力するフリップ・フロップを備えた物理乱数発生器において、前記フリップ・フロップに入力される入力信号の位相を調整するディレーとセレクターからなる可変ディレーを前記各エッジ検出回路の前段または後段に設け、前記フリップ・フロップから出力される“０”または“１”がそれぞれ５０％に収束するように当該フリップ・フロップの出力を前記可変ディレーにフィードバックするフィードバック回路を設けて構成される。

【０００７】

また、本発明のうち請求項３に係る発明は、前記積分回路の抵抗の後段にＦＥＴを当該積分回路のキャパシタと並列に付加して構成される。

【０００８】

また、本発明のうち請求項４に係る発明は、前記積分回路の抵抗に代えて定電流回路を設けて構成される。

【０００９】

さらに、本発明のうち請求項５に係る発明は、上記物理乱数発生器を２個以上並列接続し、前記各物理乱数発生器に入力されたパラレル物理乱数をシリアル物理乱数に並べ替えて出力するようにして構成される。

【発明の効果】

【００１０】

本発明のうち請求項１に係る発明によれば、ディレーおよび第１セレクターを半分にしてゲート数を削減することができるので、物理乱数発生器の規模を小さくして占有面積を縮小するとともに、その消費電力を低減することが可能となる。

【００１１】

また、本発明のうち請求項２に係る発明によれば、２系統の信号ラインについて積分回路が１つで済むことに加えて、積分回路を構成する抵抗、キャパシタの誤差による位相調整範囲を狭めることができるため、可変ディレーを縮小し、ゲート数を削減することができることから、物理乱数発生器の規模を小さくして占有面積を縮小するとともに、その消費電力を低減することが可能となる。

【００１２】

また、本発明のうち請求項３に係る発明によれば、積分回路のキャパシタに充電された電荷を放電して電位を積分波形の基点に戻すことにより、積分波形の基点、ひいてはジッターの分布を安定させ、良質な乱数を生成することができる。また、積分回路のキャパシタに充電された電荷が高速に放電され、電位も高速に積分波形の基点に戻るため、乱数生成までの待ち時間が短縮されることに加え、乱数生成後に波形の電位が上がりきるのを待たずして強制的に基点まで電位を下げることができるので、さらなる時間短縮が可能となることから、乱数生成スピードを大幅に高速化することができる。

【００１３】

また、本発明のうち請求項４に係る発明によれば、積分回路を構成するキャパシタの充電時の積分波形が直線となり、ノイズに対して変調したジッターの歪みがなくなるため、乱数の質を向上させることができる。

【００１４】

さらに、本発明のうち請求項５に係る発明によれば、複数個の物理乱数発生器からなる物理乱数発生装置の乱数の質を向上させることができる。

【発明を実施するための最良の形態】

【００１５】

以下、本発明の実施形態を図面に基づいて説明する。

【００１６】

＜第１の実施形態＞

図１は本発明に係る物理乱数発生器の第１の実施形態を示す回路図、

図２は図１に示す物理乱数発生器のエッジ検出回路の詳細を示す回路図、
図３は図１に示す物理乱数発生器の動作波形を示す図である。

【００１７】

この物理乱数発生器１においては、図１および図３に示すように、抵抗Ｒおよびキャパシタ（コンデンサ）Ｃでクロック信号を積分して積分波形を出力する積分回路５と、ノイズ源６と、このノイズ源６のノイズを増幅してノイズ信号を出力するアンプ７と、積分波形とノイズ信号とをミキシングするミキサー８と、このミキサー８の出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路９とが２個ずつ設けられている。各エッジ検出回路９は、図２に示すような回路構成となっており、これらのエッジ検出回路９の後段には、図１に示すように、各エッジ検出回路９の出力信号の位相差に基づいて“０”または“１”を出力するＤタイプのフリップ・フロップ１０が設けられている。さらに、フリップ・フロップ１０の後段には、乱数をクロック信号に同期させるＤタイプのフリップ・フロップ１１が設けられている。

【００１８】

また、物理乱数発生器１の最前段には、各積分回路５に入力される入力信号の位相を調整する位相調整部２が設けられており、この位相調整部２はディレー２１、第１セレクター２２およびアップ／ダウンカウンター２３から構成されている。

【００１９】

また、フリップ・フロップ１１の出力とアップ／ダウンカウンター２３との間にはフィードバック回路３が設けられており、フリップ・フロップ１１から出力される“０”または“１”がそれぞれ５０％に収束するようにフリップ・フロップ１１の出力が位相調整部２にフィードバックされる。すなわち、フィードバック回路３は第１カウンター３１、比較器３２、第２カウンター３３、レジスター３４、比較器３５、シフトレジスター／レジスター３６、加算器３７から構成されており、第１カウンター３１および比較器３２はフィードバックの周期を乱数（２×ｍ）で生成する。また、第２カウンター３３、レジスター３４および比較器３５はフィードバックの周期（２×ｍ）中の“０”または“１”の数をカウント（ｎ）し、比較データをアップ／ダウンカウンター２３に出力して乱数の一様性を補正するフィードバック信号を出力する。さらに、シフトレジスター／レジスター３６および加算器３７は、フィードバックの周期を決める乱数（ｍ）を出力（ＯＵＴ）より取得する。これにより、フィードバック周期による乱数の質の低下（癖）を防ぐことができる。

【００２０】

さらに、位相調整部２と各積分回路５との間にはそれぞれ第２セレクター１５および第３セレクター１６が設けられているとともに、第１セレクター２２とアップ／ダウンカウンター２３との間には極性切換回路１３が設けられており、表１に示すように、アップ／ダウンカウンター２３の最上位ビットＭＳＢによって第１セレクター２２と第２セレクター１５および第３セレクター１６との入力の極性切換が行われる。

【００２１】

【表１】

アップ/ダウンカウンター	SELECT	第1セレクターのアドレス	第2セレクターの出力	第3セレクターの出力	相対的な時間差
1Fh	1	1Fh	0(A)	P-1(A)	P
1Eh		1Eh	0(A)	P-2(A)	P-1
：		：	：	：	：
02h		02h	0(A)	2(A)	3
01h		01h	0(A)	1(A)	2
00h		00h	0(A)	0(A)	1
3Fh	0	00h	0(B)	-1(B)	0
3Eh		01h	1(B)	-1(B)	-1
：		02h	2(B)	-1(B)	-2
：		：	：	：	：
22h		：	：	：	：
21h		1Eh	P-2(B)	-1(B)	-P+2
20h		1Fh	P-1(B)	-1(B)	-P+1

【００２２】

したがって、２系統の信号ラインに応じた２個のディレーおよびセレクターを必要とする従来の物理乱数発生器と比べて、ディレー２１および第１セレクター２２を半分にしてゲート数を削減することができるので、物理乱数発生器１の規模を小さくして占有面積を縮小し、その消費電力を低減することが可能となる。

【００２３】

＜第２の実施形態＞

図４は本発明に係る物理乱数発生器の第２の実施形態を示す回路図である。

【００２４】

この物理乱数発生器１においては、図４に示すように、抵抗Ｒおよびキャパシタ Ｃでクロック信号を積分して積分波形を出力する積分回路５が１つ設けられているとともに、ノイズ源６と、このノイズ源６のノイズを増幅してノイズ信号を出力するアンプ７と、積分波形とノイズ信号とをミキシングするミキサー８と、このミキサー８の出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路９とが２個ずつ設けられている。これらのエッジ検出回路９の後段には、各エッジ検出回路９の出力信号の位相差に基づいて“０”または“１”を出力するＤタイプのフリップ・フロップ１０が設けられており、フリップ・フロップ１０の後段には、乱数をクロック信号に同期させるＤタイプのフリップ・フロップ１１が設けられている。

【００２５】

また、フリップ・フロップ１０と各エッジ検出回路９との間（各エッジ検出回路９の後段）にはそれぞれ、ディレーとセレクターからなる可変ディレー１９が設けられており、フリップ・フロップ１０に入力される入力信号の位相を調整することができる。

【００２６】

さらに、フリップ・フロップ１１の出力とアップ／ダウンカウンター２３との間にはフィードバック回路３が設けられており、フリップ・フロップ１１から出力される“０”または“１”がそれぞれ５０％に収束するようにフリップ・フロップ１１の出力が可変ディレー１９にフィードバックされる。

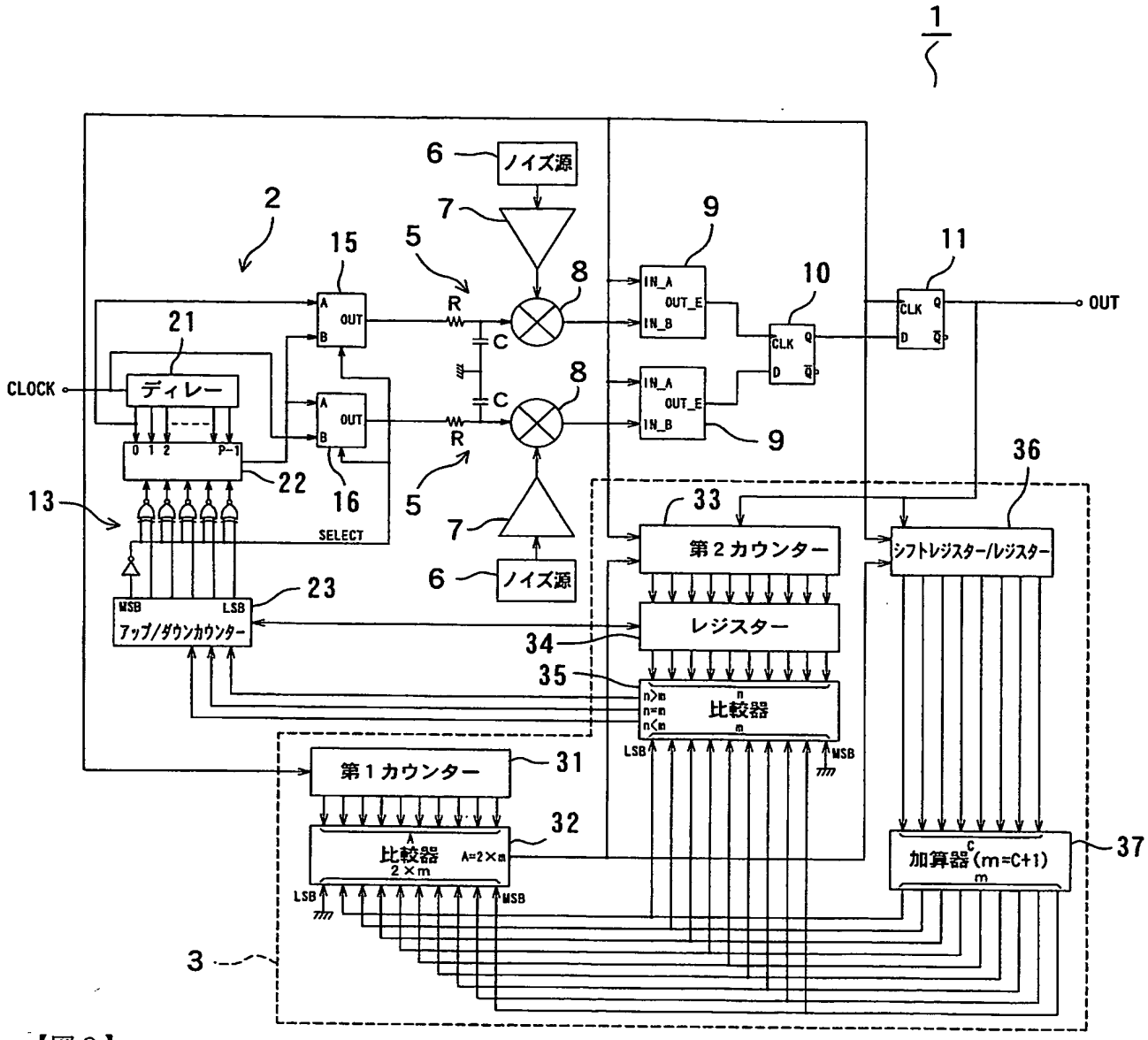
【００２７】

したがって、２系統の信号ラインについて積分回路５が１つで済むことに加えて、積分回路５を構成する抵抗Ｒ、キャパシタＣの誤差による位相調整範囲を狭めることができるため、ディレーとセレクターからなる可変ディレー１９を縮小し、ゲート数を削減することができることから、物理乱数発生器１の規模を小さくして占有面積を縮小し、その消費電力を低減することが可能となる。

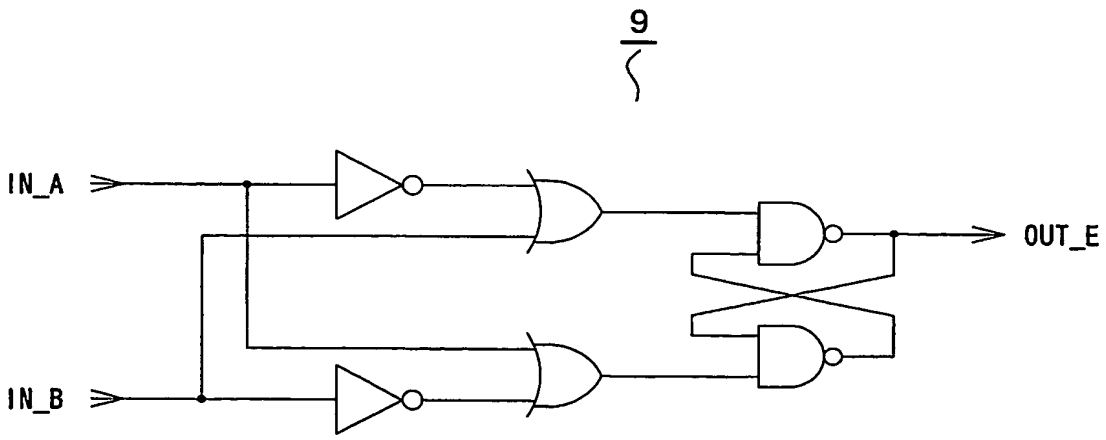
【００２８】
＜その他の実施形態＞
なお、上述した第２の実施形態において、図５に示すように、積分回路５の抵抗Ｒの後段にＦＥＴ（電界効果トランジスタ）１７をキャパシタＣと並列に付加してもよい。この場合は、図６に示すように、積分回路５のキャパシタＣに充電された電荷を放電して電位を積分波形の基点に戻すことにより、積分波形の基点が常に安定し、その結果としてジッターの分布も安定する。さらに、ジッターの分布が安定することは良質な乱数を生成することにつながる。また、乱数生成は電位が基点に戻るまで待たなければならないが、積分回路５のキャパシタＣに充電された電荷が高速に放電され、電位も高速に積分波形の基点に戻るため、乱数生成までの待ち時間を短縮することができる。それに加え、乱数生成後に波形の電位が上がりきるのを待たずして強制的に基点まで電位を下げることができるので、さらなる時間短縮が可能となる（乱数生成したら、すぐに電位を基点まで戻せる）。これにより、乱数生成スピードを大幅に高速化することができる。同様に、上述した第１の実施形態において、各積分回路５の抵抗Ｒの後段にＦＥＴ１７をキャパシタＣと並列に付加することもできる。
【００２９】
また、上述した第２の実施形態において、図７に示すように、積分回路５の抵抗Ｒに代えて定電流回路１８を設けても構わない。この場合は、図８に示すように、キャパシタＣの充電時の積分波形が直線となり、ノイズに対して変調したジッターの歪みがなくなるため、乱数の質が向上する。同様に、上述した第１の実施形態において、各積分回路５の抵抗Ｒに代えて定電流回路１８を設けることも可能である。
【００３０】
また、図９に示すように、上述した物理乱数発生器１をｋ個（ｋは２以上）並列接続し、各物理乱数発生器１に入力されたパラレル物理乱数をｋ個のシリアル物理乱数に並べ替え、排他的論理和（ＸＯＲ）素子を介して出力することにより、複数個の物理乱数発生器１からなる物理乱数発生装置の乱数の質を向上させることもできる。
【００３１】
また、上述した第１および第２の実施形態においては、乱数発生用のフリップ・フロップとしてＤタイプのフリップ・フロップを用いた場合について説明したが、本発明ではこれに限定されるわけではなく、これと同等の機能を有するフリップ・フロップであれば代用することができる。
【００３２】
また、上述した第２の実施形態においては、図４に示すように、ディレーとセレクターからなる可変ディレー１９をエッジ検出回路９の後段に設けた場合について説明したが、可変ディレー１９をエッジ検出回路９の前段に設けてもよい。
【図面の簡単な説明】
【００３３】
【図１】本発明に係る物理乱数発生器の第１の実施形態を示す回路図である。
【図２】図１に示す物理乱数発生器のエッジ検出回路の詳細を示す回路図である。
【図３】図１に示す物理乱数発生器の動作波形を示す図である。
【図４】本発明に係る物理乱数発生器の第２の実施形態を示す回路図である。
【図５】積分回路の別の例を示す回路図である。
【図６】図５に示す積分回路を用いた物理乱数発生器の動作波形を示す図である。
【図７】積分回路のさらに別の例を示す回路図である。
【図８】図７に示す積分回路を用いた物理乱数発生器の動作波形を示す図である。
【図９】本発明に係る物理乱数発生装置の一実施形態を示す回路図である。
【符号の説明】
【００３４】
１……物理乱数発生器
５……積分回路

６……ノイズ源
７……アンプ
８……ミキサー
９……エッジ検出回路
１０、１１……フリップ・フロップ
２……位相調整部
１５……第２セレクター
１６……第３セレクター
２１……ディレー
２２……第１セレクター
２３……アップ／ダウンカウンター
３……フィードバック回路
１７……ＦＥＴ
Ｒ……抵抗
Ｃ……キャパシタ
１８……定電流回路

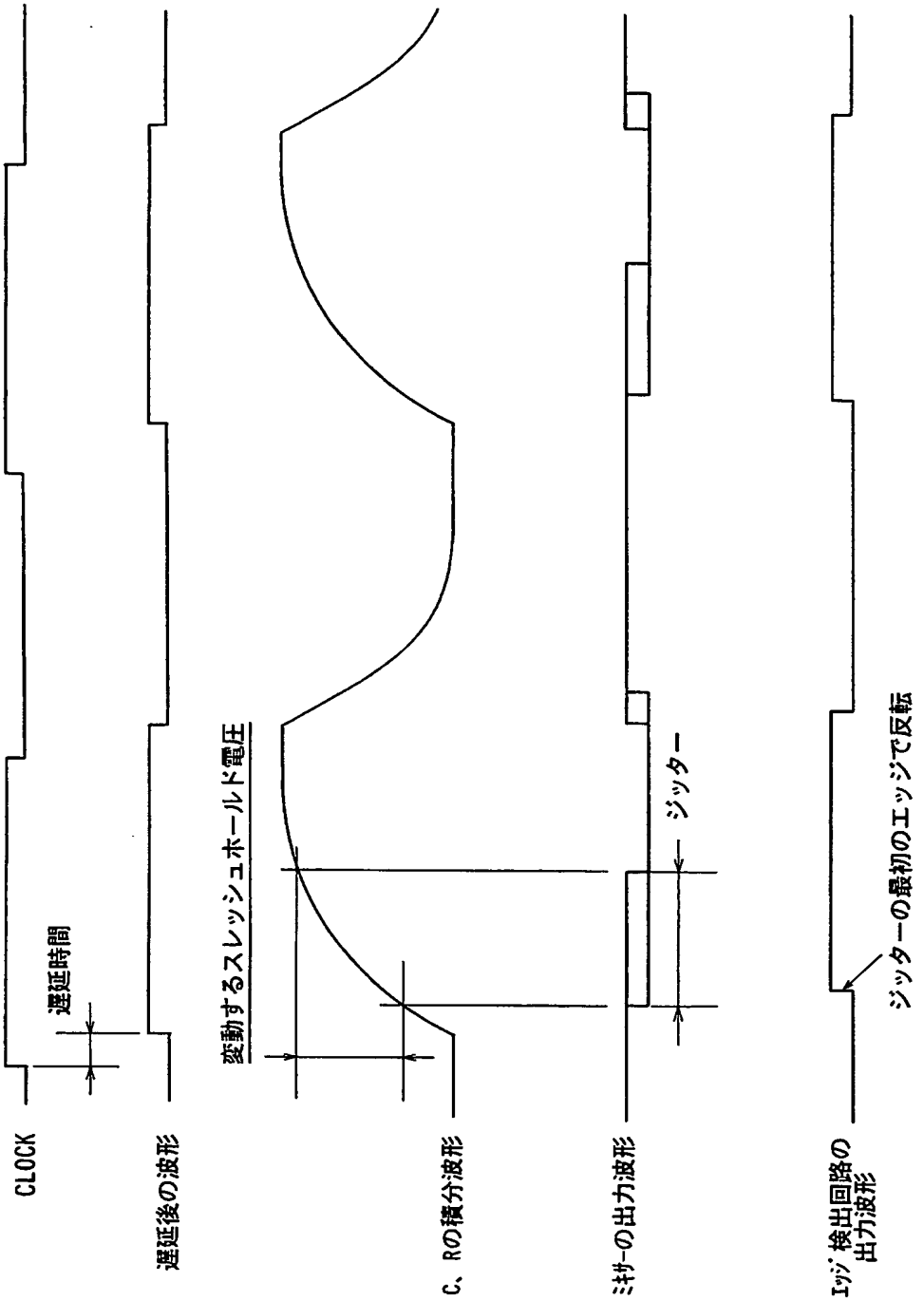
【書類名】図面
【図１】


1
2
3
5
6
ノイズ源
7
8
9
10
11
15
16
21
22
23
13
CLOCK
ディレー
SELECT
OUT
R
C
IN_A
IN_B
OUT_E
CLK
D
Q
MSB
LSB
アップ/ダウンカウンター
第１カウンター
第２カウンター
レジスター
比較器
2×m
A=2×m
n>m
n=m
n<m
31
32
33
34
35
36
37
シフトレジスター/レジスター
加算器 (m=C+1)

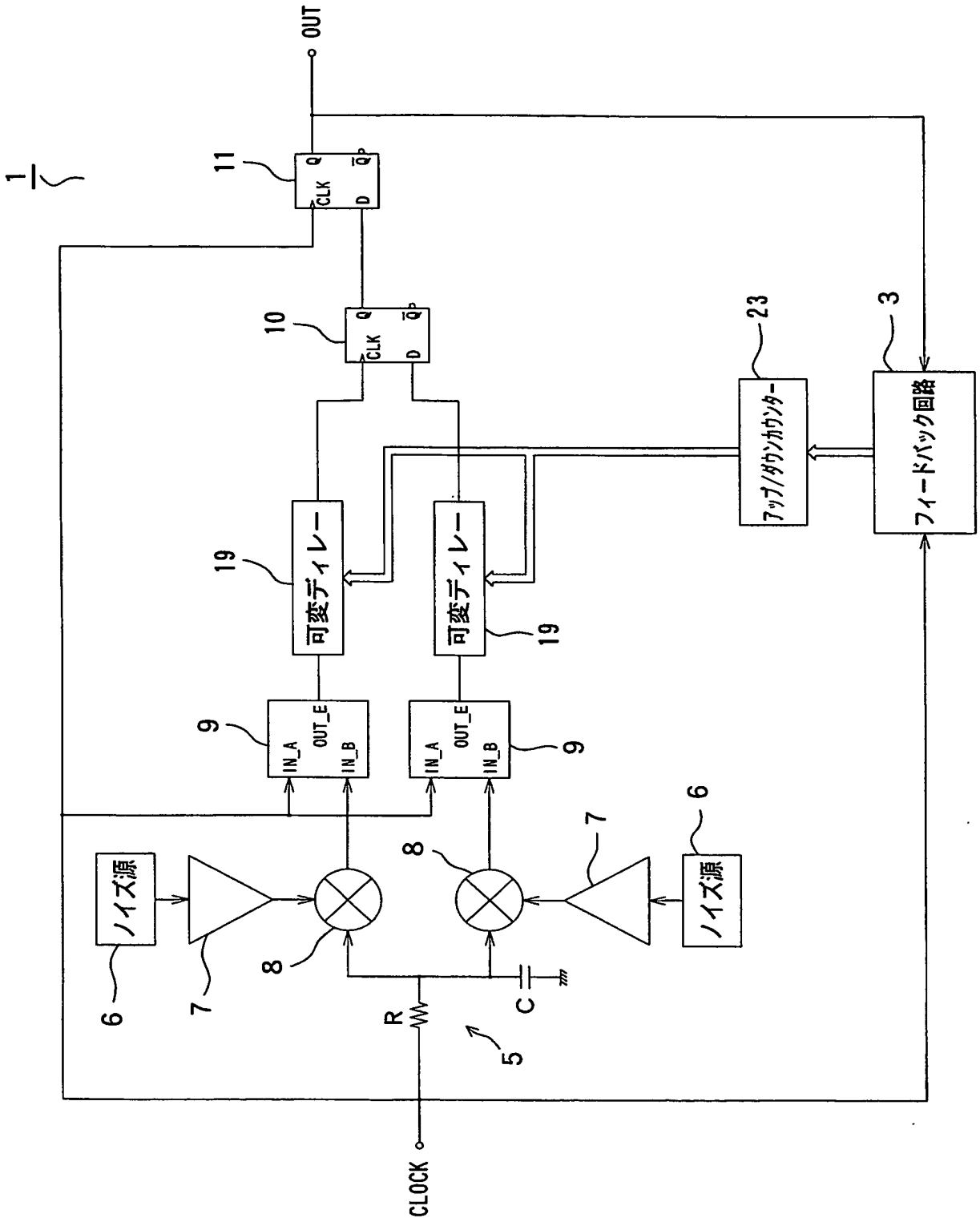
【図２】


9
IN_A
IN_B
OUT_E

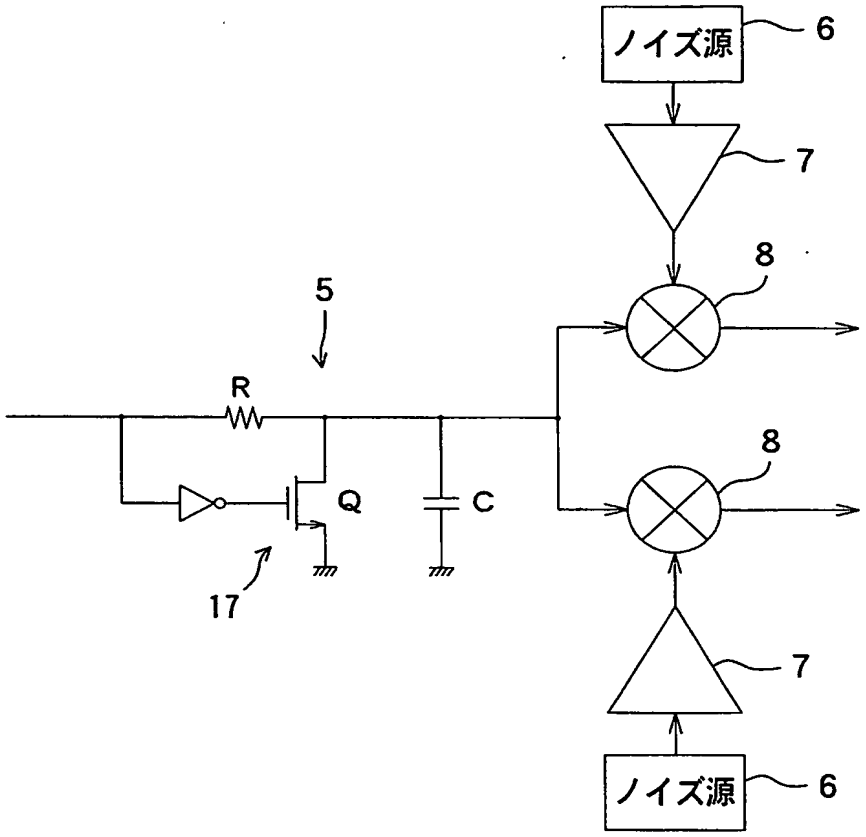
【図３】


CLOCK
遅延時間
遅延後の波形
変動するスレッシュホールド電圧
C、Rの積分波形
ジッター
ﾐｷｻｰの出力波形
ｴｯｼﾞ検出回路の出力波形
ジッターの最初のエッジで反転

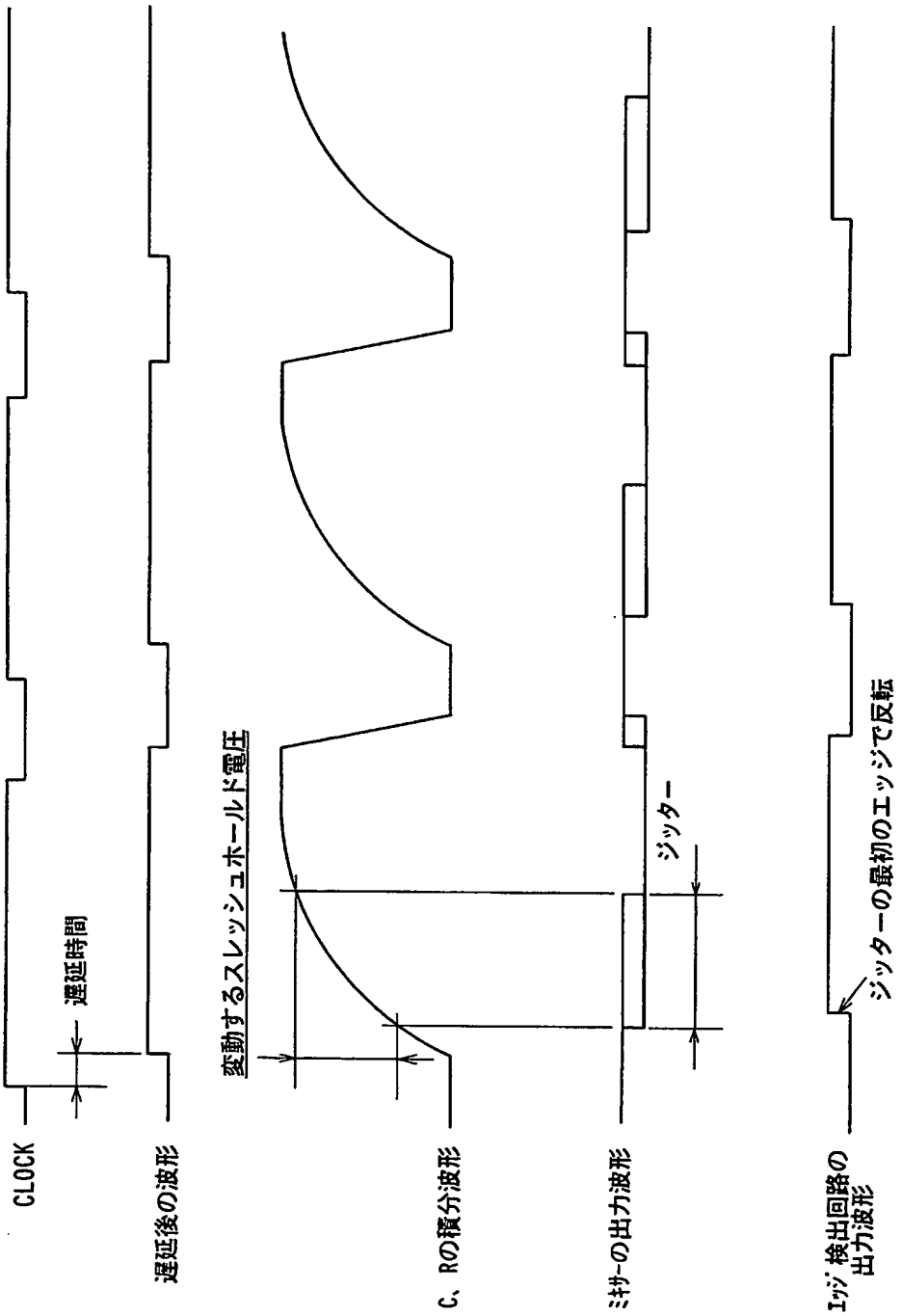
【図４】


OUT
1
11
CLK
Q
D
10
23
3
アップ/ダウンカウンター
フィードバック回路
19
可変ディレー
19
9
IN_A
OUT_E
IN_B
6
ノイズ源
7
8
R
C
5
CLOCK

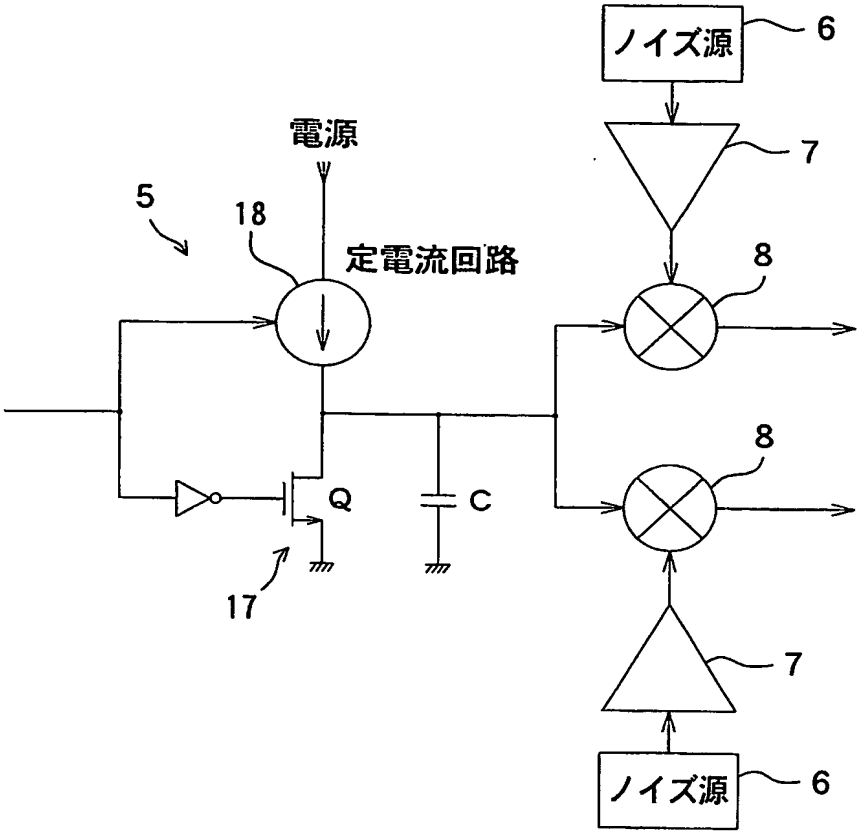
【図５】



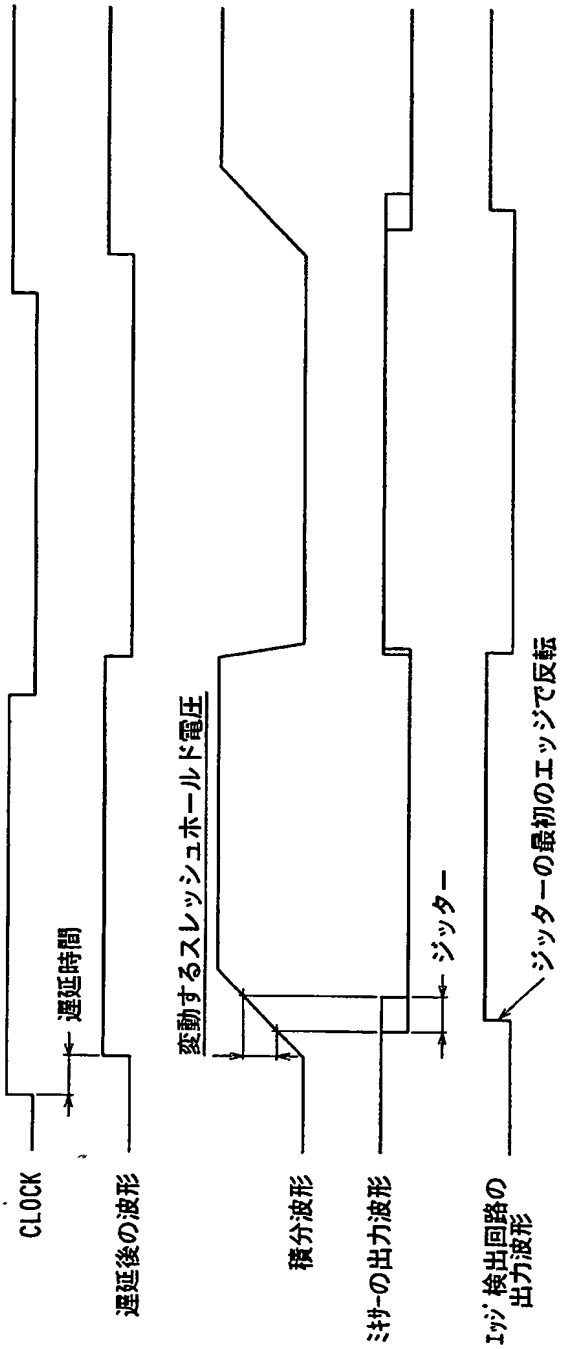
【図６】


CLOCK
遅延時間
遅延後の波形
変動するスレッシュホールド電圧
C、Rの積分波形
ジッター
ﾐｷｻｰの出力波形
ｴｯｼﾞ検出回路の出力波形
ジッターの最初のエッジで反転

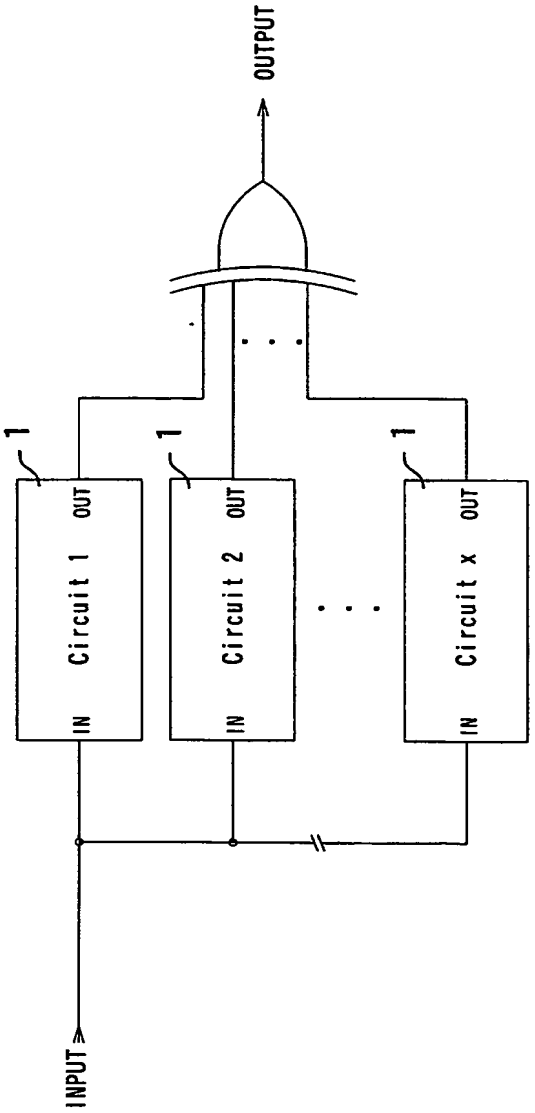
【図７】



【図８】


CLOCK
遅延時間
遅延後の波形
変動するスレッシュホールド電圧
積分波形
ジッター
ミキサーの出力波形
エッジ検出回路の出力波形
ジッターの最初のエッジで反転

【図９】



【書類名】要約書
【要約】
【課題】暗号化通信、ゲームなど各種の用途に用いるに好適な物理乱数発生器において、占有面積を縮小し、消費電力を低減する。
【解決手段】各積分回路５の前段にそれぞれ第２セレクター１５および第３セレクター１６を設け、アップ／ダウンカウンター２３の最上位ビットによって第１セレクター２２と第２セレクター１５および第３セレクター１６との入力の極性切換を行う極性切換回路１３を設ける。これにより、ディレー２１および第１セレクター２２を半分にしてゲート数を削減できる。また、積分回路５の抵抗Ｒの後段にＦＥＴをキャパシタＣと並列に付加すれば、乱数の質が向上し、動作スピードが高速になる。さらに、積分回路５の抵抗Ｒに代えて定電流回路を設けると、乱数の質が向上する。
【選択図】図１

認定・付加情報

特許出願の番号	特願２００３－２９４１０１
受付番号	５０３０１３５２９２８
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　８月１９日

＜認定情報・付加情報＞

【提出日】　平成15年 8月18日

特願２００３－２９４１０１

出　願　人　履　歴　情　報

識別番号　　［０００２３７７２１］

１．変更年月日　　２００１年　１月１６日
　［変更理由］　　名称変更
　　住　所　　東京都港区新橋５丁目３６番１１号
　　氏　名　　エフ・ディー・ケイ株式会社

２．変更年月日　　２００３年　８月１３日
　［変更理由］　　名称変更
　　住　所　　東京都港区新橋５丁目３６番１１号
　　氏　名　　ＦＤＫ株式会社